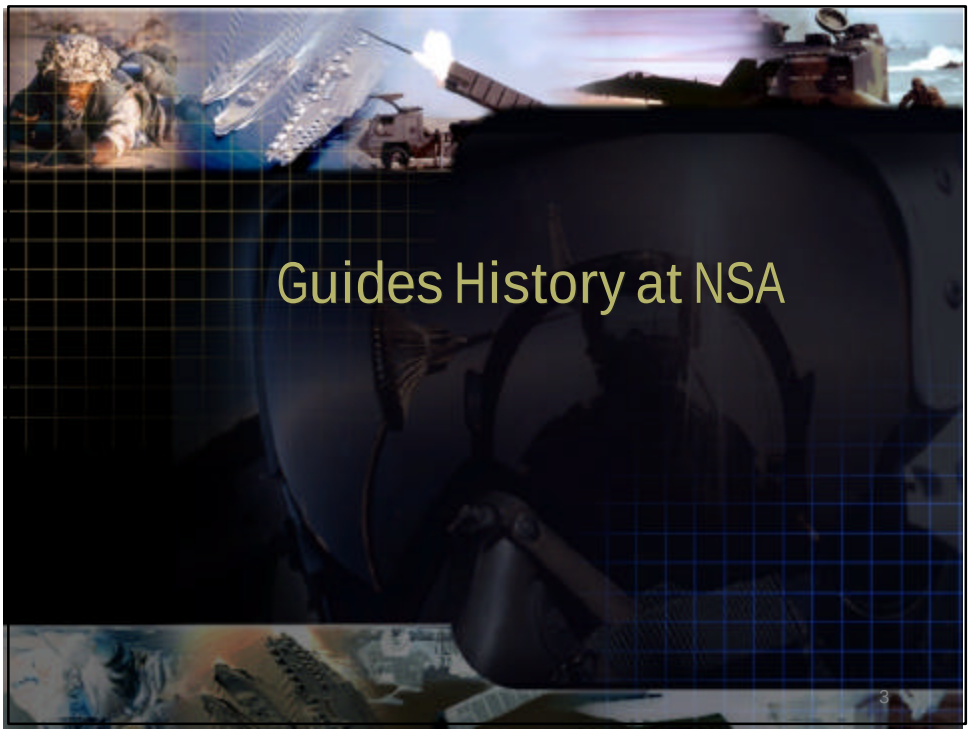
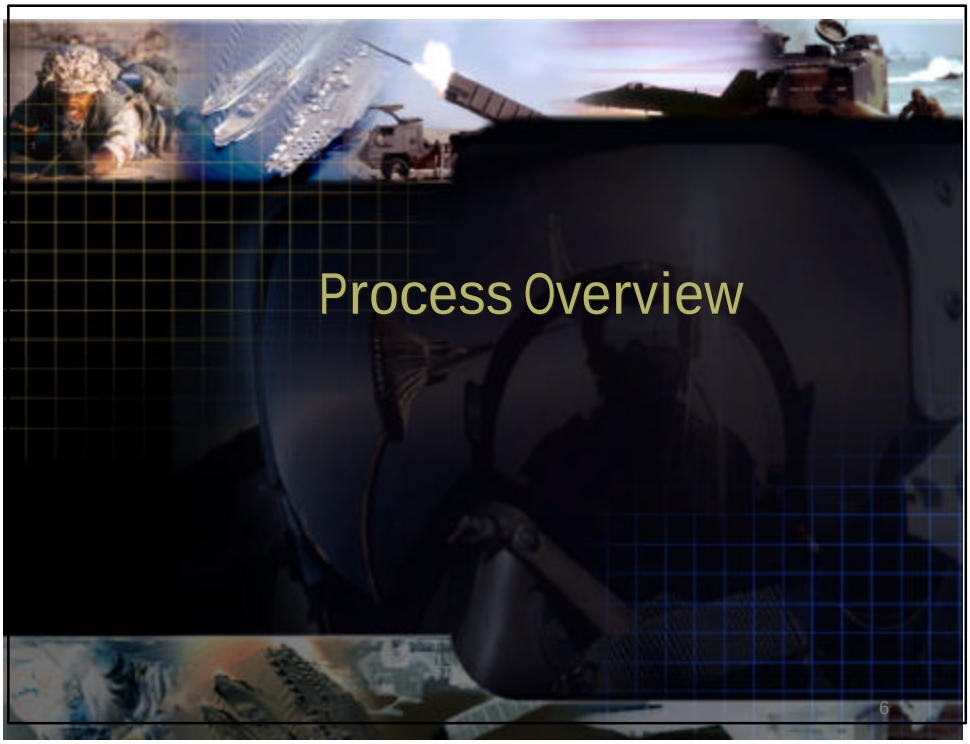

Producing Quality Configuration Guides – A NSA Perspective
Trent Pitsenbarger
NSA
Trent@TheCouch.ncsc.mil
1


Road Map
Guides history at NSA
Guide development - business process overview
Content development – security checklist issues
Forecast [wish list] for the future
2


Guides History at NSA
3


History
Circa 1996: Problem – How do we service all the customer requests?
Solution: Configuration Guides
Customers:
Initially - A few select customers
Later
Win NT OS and Applications CD
Audience: ~10,000 Government users and their contractors
Currently
Web presence
Audience: The entire world
4


Current Status
38 Guides Published on www.nsa.gov
Consulted on many others
Partners:
CIS
Vendors
Other Govt. agencies
5


Process Overview
6

Our Goals

- Deliver the best product possible
- Reduce the number of calories an admin must expend

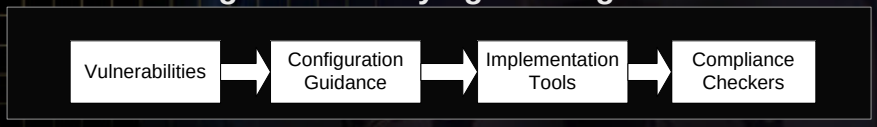
7

Community Involvement

8

The “Big Picture”

- **The “Big Picture” – tying it all together**

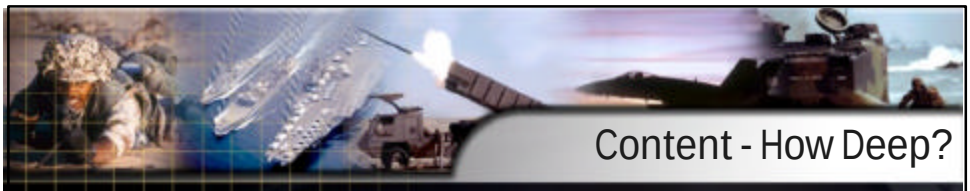


- **Nirvana: Automatic translation**

9

Content Development

10

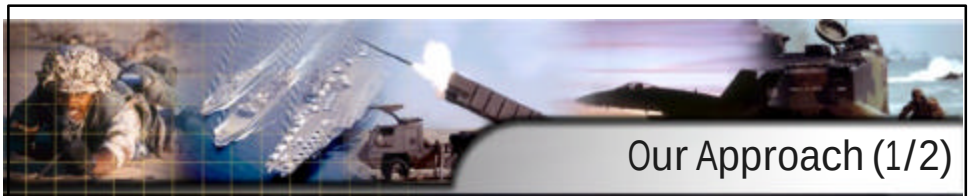


Content - How Deep?

- **Level 1: ID the security relevant features**
  - ***Little value to the reader – not acceptable***
- **Level 2: ID the security features along with recommendations**
  - ***Better, but still lacking***
- **Level 3: Identification of the security features along with recommendations, interdependences, lessons learned**

Target audience – administrator who basically understands the app but needs to understand the security aspects

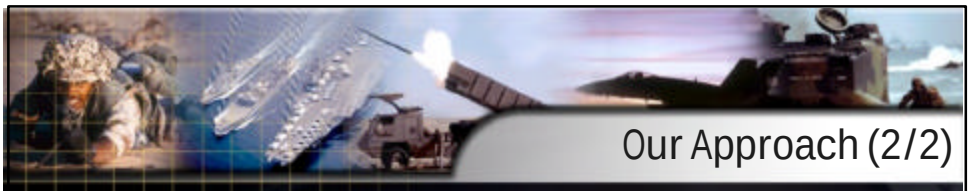
11



Our Approach (1/2)

- **Study**
  - ***Known threats, vulnerabilities***
  - ***Take max. advantage of what has already been written***
- **Explore**
  - ***Exercise the security model***
  - ***Take copious notes***
- **Understand -- and keep taking notes**
- **Write**
  - ***10% of the task if the writer truly understands***
  - ***Don't forget the target audience***

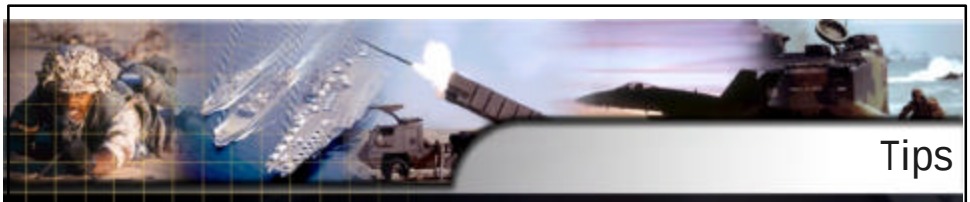
12



Our Approach (2/2)

- **Test and verify**
  - ***Do the various guides play together***
  - ***Does the document focus on security***
  - ***Is the document consistent***
  - ***Are we as prescriptive as practical***
  - ***Do we cover the security relevant issues***
  - ***Did we hit the target audience***

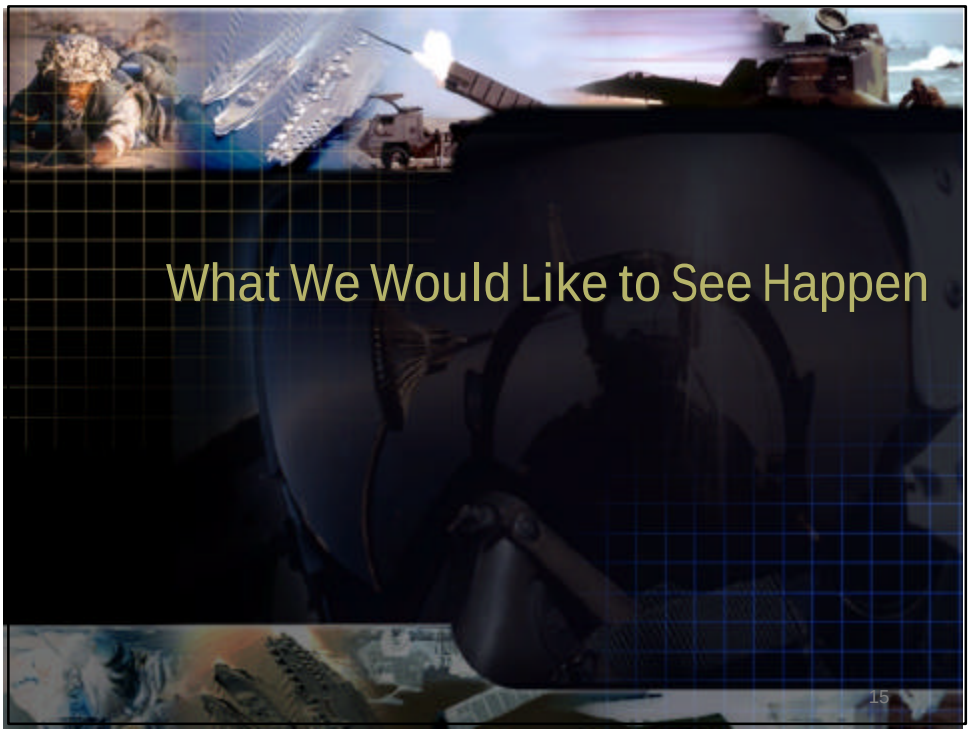
13

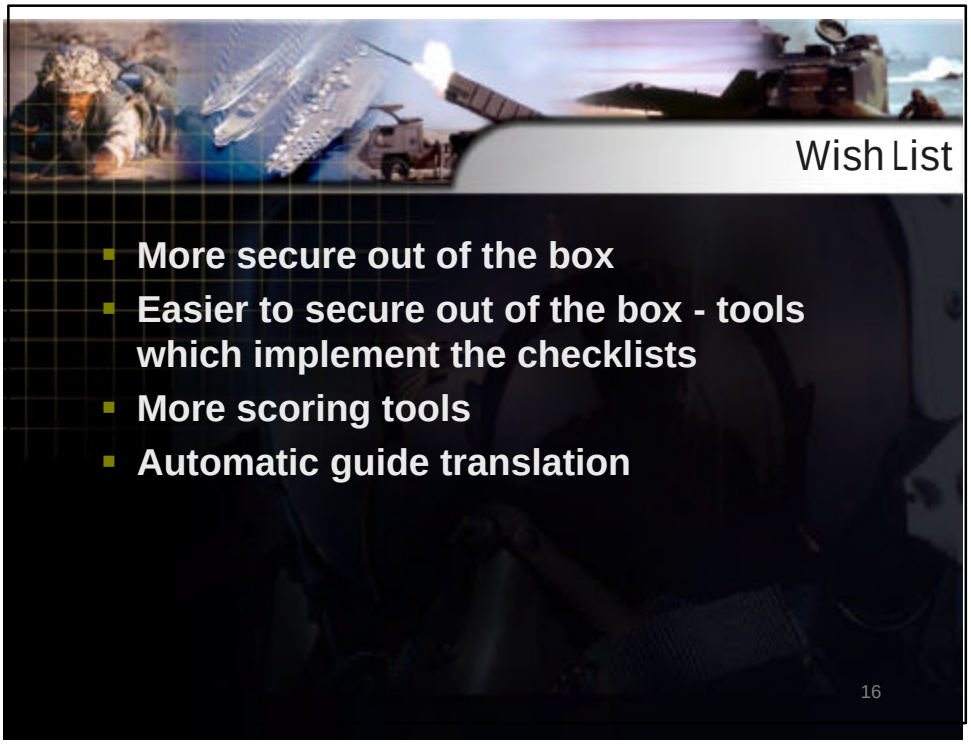


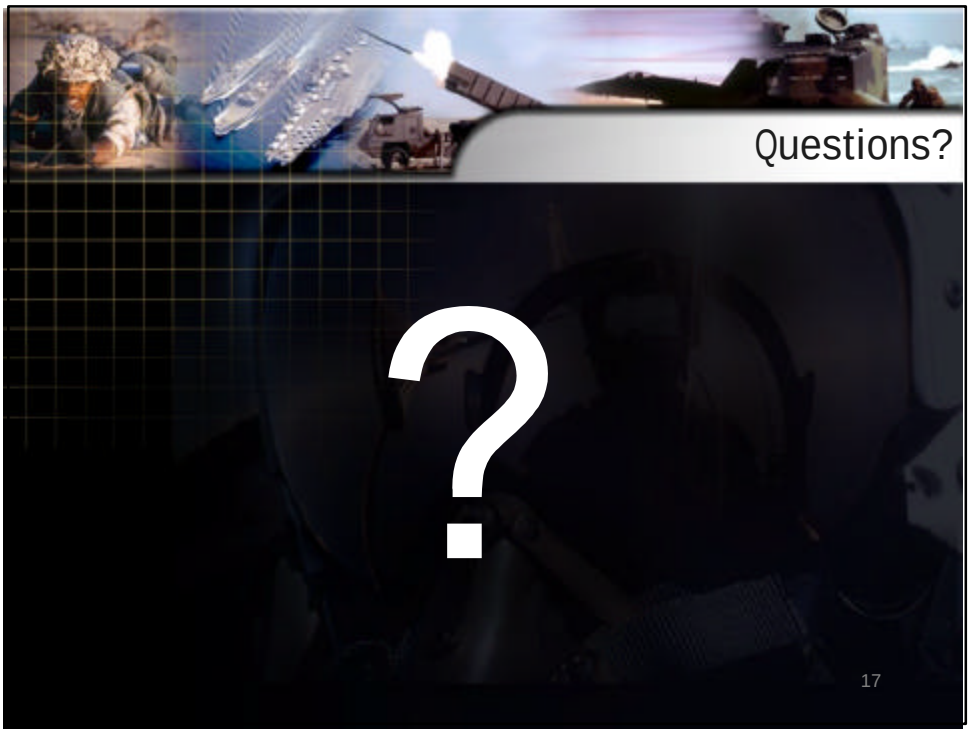
Tips

- **Use some means of rapid recovery during development**
- **Always remember the target audience**
- **Remember you are writing a *security* guide**
- **Be meticulous in final test**

14


What We Would Like to See Happen
15


Wish List
More secure out of the box
Easier to secure out of the box - tools which implement the checklists
More scoring tools
Automatic guide translation
16


Questions?
?
17